Brookhaven National Laboratory

Safeguards & Security

Stand Down

PHYSICAL SECURITY

August 1999

Joseph Musorrafiti

Brookhaven Science Associates
U.S. Department of Energy

BROOKHAVEN NATIONAL LABORATORY

Physical Security

- Protect Personnel
- Prevent or detect unauthorized access to facilities, material, or documents
- Protect against espionage, sabotage and theft
- Respond to any such acts should they occur

Security Areas

BNL has four security areas

- High Flux Beam Reactor (HFBR)
- Medical Reactor
- Dept. Advanced Technology
- Police Headquarters

Security Areas (Con't.)

There are an additional 12 buildings with security equipment for property protection or safety.

If you desire physical security upgrades, contact us and we will survey the area and provide advice and an estimate for equipment if needed.

Site Signaling System

The Site Signaling System is being upgraded. Most of the property protection areas are on the new system and the upgrade will be completed by 9/30/99.

The system was replaced because it is not Y2K compliant and could not meet the new specifications for the DOE standard badge.

Site Signaling System (Con't.)

There are many improvements over the existing system:

- Speed - Mosler 600 BAUD - Lantek 375K BAUD
- Alarms report < 1 sec
- Video call-up < 1 sec on reported alarm
- Video on existing communication lines (10 frames per sec)
- Support DOE Standard Badge
- Customized Reports
- Supports multiple technologies - magnetic stripe, proximity, hand geometry, bar code, fingerprint, iris, etc. (We only use magnetic stripe and bar code at this time.)

Technical Surveillance Countermeasures (TSCM)

- Systematic and effective measures for detection and/or nullification of technical surveillance penetrations and hazards.
- There are two secure conference rooms at BNL. It is important to follow procedures. If the room is compromised, it could be months before it is re-certified.

TEMPEST

- Control of compromising emanations from telecommunications and automated information systems equipment.
- Compromising emanations are unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled or otherwise processed by telecommunications and automated information systems equipment.